CLAIMS

That which is claimed:

1. A method of processing communication traffic, comprising:

detecting an anomaly in the communication traffic;

applying a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

determining a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic.

2. The method of Claim 1, wherein determining the second blocking measure B comprises:

applying a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

enforcing the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic.

3. The method of Claim 2, further comprising:

determining a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic.

4. The method of Claim 2, wherein determining the second blocking measure B further comprises:

applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

enforcing the logical combination (A & B) if the logical combination (A & B) stops the anomalous traffic.

5. The method of Claim 4, further comprising:

determining a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) stops the anomalous traffic.

6. The method of Claim 4, further comprising:

determining a second blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) does not stop the anomalous traffic.

7. The method of Claim 1, wherein detecting an anomaly in the communication traffic comprises:

detecting a pattern in a value of at least one protocol field associated with the communication traffic.

8. The method of Claim 1, wherein detecting an anomaly in the communication traffic comprises:

detecting that a flow rate of the anomalous traffic exceeds a threshold.

9. A method of processing communication traffic, comprising:

detecting an anomaly in the communication traffic;

applying a first blocking measure A to the anomalous traffic that reduces a flow rate of the anomalous traffic below a threshold; and

determining a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure to the anomalous traffic reduces the flow rate of the anomalous traffic below the threshold.

10. A system for processing communication traffic, comprising:

means for detecting an anomaly in the communication traffic;

means for applying a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

means for determining a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic.

11. The system of Claim 10, wherein the means for determining the second blocking measure comprises:

means for applying a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

means for enforcing the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic.

12. The system of Claim 11, further comprising:

means for determining a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic.

13. The system of Claim 11, wherein the means for determining the second blocking measure B further comprises:

means for applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

means for enforcing the logical combination (A & B) if the logical combination (A & B) stops the anomalous traffic.

14. The system of Claim 13, further comprising:

means for determining a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) stops the anomalous traffic.

15. The system of Claim 13, further comprising:

means for determining a second blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) does not stop the anomalous traffic.

16. The system of Claim 10, wherein the means for detecting an anomaly in the communication traffic comprises:

means for detecting a pattern in a value of at least one protocol field associated with the communication traffic.

17. The system of Claim 10, wherein the means for detecting an anomaly in the communication traffic comprises:

means for detecting that a flow rate of the anomalous traffic exceeds a threshold.

18. A system of processing communication traffic, comprising:

means for detecting an anomaly in the communication traffic;

means for applying a first blocking measure A to the anomalous traffic that reduces a flow rate of the anomalous traffic below a threshold; and

means for determining a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic reduces the flow rate of the anomalous traffic below the threshold.

19. A computer program product for processing communication traffic, comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to detect an anomaly in the communication traffic;

computer readable program code configured to apply a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

computer readable program code configured to determine a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic.

20. The computer program product of Claim 19, wherein the computer readable program code configured to determine the second blocking measure comprises:

computer readable program code configured to apply a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

computer readable program code configured to enforce the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic.

21. The computer program product of Claim 20, further comprising:

computer readable program code configured to determine a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic.

22. The computer program product of Claim 20, wherein the computer readable program code configured to determine the second blocking measure B further comprises:

computer readable program code configured to apply a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

computer readable program code configured to enforce the logical combination (A & B) if the logical combination (A & B) stops the anomalous traffic.

23. The computer program product of Claim 22, further comprising:

computer readable program code configured to determine a third blocking measure C such that application of a logical combination of (A & B) and the third

blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) stops the anomalous traffic.

24. The computer program product of Claim 22, further comprising:

computer readable program code configured to determine a second blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) does not stop the anomalous traffic.

25. The computer program product of Claim 19, wherein the computer readable program code configured to detect an anomaly in the communication traffic comprises:

computer readable program code configured to detect a pattern in a value of at least one protocol field associated with the communication traffic.

26. The computer program product of Claim 19, wherein the computer readable program code configured to detect an anomaly in the communication traffic comprises:

computer readable program code configured to detect that a flow rate of the anomalous traffic exceeds a threshold.

27. A computer program product for processing communication traffic, comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to detect an anomaly in the communication traffic;

computer readable program code configured to apply a first blocking measure A to the anomalous traffic that reduces a flow rate of the anomalous traffic below a threshold; and

computer readable program code configured to determine a second blocking measure B such that application of a logical combination of the first blocking measure

A and the second blocking measure B to the anomalous traffic reduces the flow rate of the anomalous traffic below the threshold.